UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,
Plaintiff,

16-CR-65-V

-v-

JOSHUA ZAK,
Defendant.

DECISION AND ORDER

This case was referred to the undersigned by the Hon. Lawrence J. Vilardo, in accordance with 28 U.S.C. § 636(b)(1), for all pretrial matters and to hear and report on dispositive motions. Dkt. #7.

PRELIMINARY STATEMENT

The defendant, Joshua Zak ("the defendant"), is charged in a five-count Indictment with violations of Title 18 U.S.C. Sections 2252A(a)(2)(A), 2252A(a)(5)(B) and 2252A(b)(2). Dkt. #6. Currently before the Court is defendant's onmibus discovery motion. Dkt. #14. The government has filed a response in opposition to this motion along with a request for reciprocal discovery. Dkt. #21.

DISCUSSION AND ANALYSIS

Discovery and Inspection

The defendant demands discovery and inspection of numerous items. Dkt. #14, pp.25-27. The government responds that it has provided the defendant with all

discoverable information and is in compliance with the requirements of Rule 16. Dkt. #21, p.39. The government opposes defendants' requests as detailed below.

Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure requires the government to permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody or control and: (1) the item is material to preparing the defense; (2) the government intends to use the item in its case-in-chief at trial; or (3) the item was obtained from or belongs to the defendant. An exception is made for "reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case. Fed. R. Cr. P. 16(a)(2).

Evidence is material under Rule 16 "if it could be used to counter the government's case or to bolster a defense." *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993). Materiality requires "more than that the evidence in question bears some abstract logical relationship to the issues in the case." *United States v. Maniktala*, 934 F.2d 25, 28 (2d Cir. 1991). "There must also be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." *Id.* It is the defendant's burden to make a *prima facie* showing that documents sought under the Rule are material to his defense. *United States v. Rigas*, 258 F. Supp.2d 299, 307 (S.D.N.Y. 2003).

Documents relating to the DOJ's review and approval process for the continued operation of the website

The defendant seeks all documents or other records demonstrating the FBI's compliance with the DOJ's review and approval process for establishing an online undercover facility in the Playpen investigation. Dkt. #14, p.26.

The government responds that these documents are privileged and immaterial to the defense of this indictment. Dkt. #21, p.41. Moreover, the government argues that they are protected by Rule 16(a)(2) of the Federal Rules of Criminal Procedure. Dkt. #21, pp.41-41.

The defendant has not suggested any basis for the disclosure of this information. Moreover, the court has determined in its accompanying report, recommendation and order that defendant's access of the website was completely voluntary and the government's conduct in maintaining access to the site for a limited period was not outrageous. *See, e.g., United States v. Vortman*, No. 16-cr-210, 2017 WL 1493100 (N.D. Cal. April 26, 2017); *United States v. Kim*, 16-CR-191, 2017 WL 394498 (E.D.N.Y. Jan. 27, 2017). Accordingly, this request for discovery is denied.

Screen shots of the homepage before and after February 19, 2015 and records to substantiate the claim that the website could not be located using a conventional internet browser.

The defendant seeks copies of screen shots of the home page as it existed before and after February 19, 2015, and records of any efforts the government

made to substantiate its claim that the website could not be located using a conventional internet browser or other ordinary search methods, including any records documenting the FBI's knowledge that the address was publicly available on at least two websites, as evidence of misrepresentations that would support a *Franks* hearing. Dkt. #14, p.27. The defendant also intends to use this information to move to suppress on the ground that the NIT warrant was an anticipatory warrant for which the necessary "triggering event" never transpired. Dkt. #14, p.27.

The government responds that other district courts have found that any purported misrepresentations in the warrant application regarding the home page or the accessibility of the website were insufficient to alter the probable cause finding and that the NIT warrant is a valid anticipatory warrant. Dkt. #21, pp.42-44.

In light of the fact that this court has determined in its accompanying report, recommendation and order that the NIT warrant was supported by probable cause regardless of whether the image presented was that of "two partially clothed prepubescent females with their legs spread apart" or "a single prepubescent female wearing fishnet stockings and posed in a sexually suggestive manner" and that there is no evidence to suggest that the agent engaged in a deliberate falsehood or reckless disregard for the truth when he described the images on the homepage as of February 18, 2015, the request for the screen shots of the homepage is denied as immaterial to the defendant's request for a *Franks* hearing. *See United States v. Gaver*, No. 3:16-CR-88, 2017 WL 1134814, at *5 (S.D. Ohio Mar. 27, 2017) (collecting cases concluding that

there was no need for a *Franks* hearing regarding image on homepage). Similarly, given the court's determination that it was improbable that an individual would register an account using a fake email account as directed by the website and after being warned not to post information that could be used to identify the user without an understanding of the contents of the site, it is immaterial to the defendant's request for a *Franks* hearing whether the location of the website was publicly available on other websites. *See United States v. Owens*, No 16-CR-38, 2016 WL 7079609, at *6 (E.D. Wis. Dec. 5, 2016), *quoting United States v. Darby*, 190 F. Supp.3d 520, 532 (E.D. Va. 2016) ("Ultimately, no matter how searchable the Tor network may be, the magistrate judge would have been justified in concluding that those individuals who registered and logged into Playpen had knowledge of its illegal content."). Finally, the Court concludes that the triggering condition of logging into the website satisfied the requirements of an anticipatory warrant because there was a fair probability that a user accessing the website was doing so to access child pornography. *See United States v. Anzalone*, 208 F. Supp.3d 358, 368-69 (D. Mass. 2016), *citing United States v. Matish*, 193 F. Supp.3d 585, 610 (E.D.Va. 2016). Accordingly, this request for discovery is denied.

Source Code for the NIT & Data Stream between Computers

The defendant seeks a copy of the source code for the NIT and a copy of the two-way data stream between his computer and the FBI's computers and server. Dkt. #14, p.27. In support of this request, defendant submits the expert declarations from another prosecution relating to the underlying investigation, *to wit, United States v.*

Michaud, 15-CR-5351 (W.D.Va.), which express concern over the security and integrity of the data discovered on users' computers due to the lack of encryption, raising issues relating to the chain of custody and reliability of data received by the FBI. Dkt. #14, p.27. According to an affidavit submitted by a forensic analyst, for example, the NIT programming or source code works by using an "exploit," which takes advantage of a software vulnerability in the Tor Browser program to circumvent the security protections in the Tor Browser, which otherwise prevents web sites from determining the true IP or MAC address of website users. Dkt. #16, p. 169. After exploiting this vulnerability, the NIT delivers a software "payload" to the target computer which collects and transmits the information about the target computer which the NIT warrant allowed to be seized, including the IP address, and a unique identifier to associate with the identifying information collected by the NIT. Dkt. #16, p.169. Thus, there are four primary components to an NIT: (1) software that generates a payload and injects a unique identifier into it; (2) the exploit that is sent to the target computer to take advantage of a software flaw in the Tor Browser; (3) the payload that is run on the target computer to extract identifying information from the target computer; and (4) an additional server component that stores and preserves the extracted information and allows investigators to access it. Dkt. #16, p.169. The forensic analyst declares that each of these components are needed to verify the accuracy of the data extracted from a target computer. Dkt. #16, p.170.

An Assistant Professor of Computer Science and Information Technology at the University of Nebraska at Kearney further explains that each of these components

must be disclosed so as to: (1) ensure that the evidence collected by the NIT is valid and accurate; (2) ensure that the NIT did not exceed what was authorized in the warrant; and (3) develop potential defenses at trial based on the NIT having compromised the security settings on the target computer, rendering it vulnerable to a host of viruses and remote attacks that would provide an alternate explanation as to why a defendant's data storage devices may contain child pornography that he did not intentionally download. Dkt. #16, pp. 179-180.

Another forensic analyst declares that all of the components must be analyzed to determine how the NIT functioned and the reliability of the data collected by it, particularly the reliability of the identifier generated by the NIT. Dkt. #16, pp.190-91.

Another declarant expresses concern that because the FBI did not use encryption to protect data transmitted between the NIT and the FBI's server, the data was vulnerable to both interception and tampering by third parties as it was transmitted over the internet. Dkt. #16, p.206.

The government responds that it will not use the NIT source code or data stream in its case in chief and argues that the information requested is not material to the defense of the indictment and there is no suggestion that the data recovered from the defendant was compromised. Dkt. #21, pp. 44-47. The government also argues that the NIT programming code is subject to a qualified law enforcement privilege, noting that disclosure could diminish the future usefulness of the code by allowing individuals to

devise measures to circumvent the NIT and evade detection. Dkt. #21, p.48. In support of its response, the government submits the declaration of Special Agent ("SA"), Daniel Alfin, originally submitted in *United States v. Matish*, 16cr16 (E.D.Va.), explaining that the NIT "consists of a single component: that is, the computer instructions delivered to the defendant's computer after he logged into Playpen that sent specific information obtained from his computer back to the FBI." Dkt. #22, ¶ 5. SA Alfin declared that "[t]hose computer instructions, and the information obtained via their execution," which defendants' experts referred to as the "payload," were "made available for review." Dkt. #22, ¶ 5. SA Alfin noted that he had "personally executed the NIT on a computer under my control and observed that it did not disable the security firewall, make any changes to the security settings on my computer or otherwise render it more vulnerable to intrusion than it already was." Dkt. #22, ¶ 9. SA Alfin further declared that the government was "willing to make available for its review the two-way network data stream showing the data sent back-and-forth between [defendant's] computer and the government-controlled computer as a result of the execution of the NIT." Dkt. #22, ¶ 15. SA Alfin declared that comparison of the information sent to the government by the NIT to the information provided in discovery would verify that the information recorded by the government was what was sent by the defendant's computer. Dkt. #22, ¶ 19. Finally, SA Alfin declared that he has "reviewed the list of unique identifiers generated during the operation and confirmed that there were in fact no duplicate identifiers generated." Dkt. #22, ¶ 26.

"The majority of courts that have considered the matter have denied motions to compel the government to disclose the NIT source code used in the Playpen investigation." *United States v. Pawlak*, No. 3:16-CR-306, 2017 WL 2362019, at *3 (N.D. Tx. May 30, 2017), *citing United States v. Gaver*, 2017 WL 1134814, at *3-4 (collecting cases). In reaching this conclusion, the courts emphasize that revealing how the NIT gained access to defendant's computer is irrelevant to defending against the criminal content discovered on that computer. *Pawlak*, 2017 WL 2362019, at *3. Moreover, courts have determined that the law enforcement privilege protects identification of the flaw within Tor that permits the government to access users' computers. *See Gaver,* 2017 WL 1134814 at *4 ("disclosure of the exploit . . . would severely compromise future investigations, and could allow others to develop countermeasures.") (collecting cases). This court agrees that the source code or exploit is immaterial to the defense of this action and, even if it were material, is protected by the law enforcement privilege. *See In re The City of New York*, 607 F.3d 923, 944 (2d Cir. 2010) (privilege applies to "law enforcement techniques and procedures" and information that would interfere with current or future investigations). Accordingly, this aspect of defendant's motion to compel is denied.

With respect to the government's objection to disclosure of the network data stream, however, the court notes that many of the cases reviewed by the court discussing disclosure of components of the NIT indicate that the government has disclosed this information voluntarily. *See, e.g., Gaver,* 2017 WL 1134814, at * 3 ("The government is willing to produce: . . . the two-way network data stream . . .); *United*

States v. McLamb, 220 F. Supp.3d 663, 675 (E.D. Va. 2016) ("government has also offered to make the two-way data stream launched by the exploit source code available for defense review); *United States v. Jean*, 2016 WL 6886871, at *2 (W.D. Ark. Nov. 22, 2016) ("Government produced the raw data that was received by the FBI from Mr. Jean's computer and internet modem . . . referred to during the hearing as the "two-way data stream."); *Darby*, Dkt. #21-2, p.6 ("The government has also provided the data that were sent from Defendant's computer to the government server."); *United Sates v. Matish*, 193 F. Supp.3d 585, 601 (E.D. Va. 2016) ("Defendant has already received . . . the two-way data stream . . ."). As SA Alfin declares, review of the two-way network data stream (which the government agreed to provide), would verify that the information recorded by the government was what was sent by the defendant's computer. Dkt. #22, ¶ 19. Accordingly, this aspect of defendant's motion to compel is granted.

Brady/Giglio & Jencks Materials

The defendant seeks disclosure of all potentially favorable evidence, including, but not limited to: statements, grand jury testimony, witnesses, books, papers, reports, photographs, handwritten notes, synopses of statements made by witnesses, or any other tangible items of evidence in the custody and control of the Government, or any Governmental agency, or agents working with, or under the supervision of the Government. Dkt. #14, p.27. The defendant also seeks disclosure of witness statements pursuant to 18 U.S.C. § 3500. Dkt. #14, p.31.

The government responds that it is fully aware of its responsibilities pursuant to *Brady* and its progeny. Dkt. #21, pp.53-54. The government represents that it will disclose Jencks Act and impeachment material regarding government witnesses earlier than required by 18 U.S.C. § 3500 and within sufficient time to permit its effective use at trial and to avoid the necessity for adjournments during trial so as to permit review of such material. Dkt. #21, p.55.

In addition to its responsibility under *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and subsequent cases, the government is required to comply with the requirements of 18 U.S.C. § 3500 with respect to production of statements of witnesses called to testify at trial, as well as with the Second Circuit Court of Appeals' holding in *United States v. Coppa*, 267 F.3d 132 (2d Cir. 2001) and *United States v. Rodriguez*, 496 F.3d 221 (2d Cir. 2007) by making timely disclosure of those materials to the defendant.

"[A]s a general rule, *Brady* and its progeny do not require immediate disclosure of all exculpatory and impeachment material upon request by a defendant." *Coppa*, 267 F.3d at 146. The prosecution is obligated to disclose and turn over *Brady* material to the defense "in time for its effective use." *Id.* at 144. With respect to impeachment material that does not rise to the level of being *Brady* material, such as *Jencks* statements, the prosecution is not required to disclose and turn over such statements until after the witness has completed his direct testimony. *See* 18 U.S.C. § 3500; Rule 26.2 Fed.R.Crim.P.; *In Re United States*, 834 F.2d 283 (2d Cir. 1987).

However, if the government has adopted a policy of turning such materials over to the defendant prior to trial, the government shall comply with that policy; or in the alternative, produce such materials in accordance with the scheduling order issued by the trial judge.

Disclosure Pursuant to FRE 404(b), 608 and 609

The defendant seeks an order compelling the government to disclose evidence pursuant to Federal Rules of Evidence 404(b), 608 and 609. Dkt. #14, pp.30-32.

The government responds that it is aware of and will comply with the notice requirements set forth in Rule 404. Dkt. #21, p.54.

Rule 404(b) FRE only requires that "the prosecution . . . provide reasonable notice in advance of trial . . . of the *general* nature of any such evidence it intends to introduce at trial" (emphasis added). In reliance upon the government's representation, defendant's request on this issue is denied as moot.

The issue of admissibility of such evidence, as raised in the defendant's request, pursuant to Rules 404(b), 608 and 609 FRE is best left to the determination of the trial judge at the time of trial.

Preservation of Rough Notes

The government is hereby directed to maintain and preserve all materials that are known by the government to exist and that constitute potential *Jencks* and Rule 16, Fed.R.Crim.P. material in this case. As the Court of Appeals for the Second Circuit admonished:

> [W]e will look with an exceedingly jaundiced eye upon future efforts to justify non-production of a Rule 16 or Jencks Act "statement" by reference to "departmental policy" or "established practice" or anything of the like. There simply is no longer any excuse for official ignorance regarding the mandate of the law. Where, as here, destruction is deliberate, sanctions will normally follow, irrespective of the perpetrator's motivation, unless the government can bear the heavy burden of demonstrating that no prejudice resulted to the defendant. . . . We emphatically second the district court's observation that any resulting costs in the form of added shelf space will be more than counterbalanced both by gains in the fairness of trials and also by the shielding of sound prosecutions from unnecessary obstacles to a conviction.

United States v. Buffalino, 576 F.2d 446, 449-50, (2d Cir.), *cert. denied*, 439 U.S. 928 (1978); *see also United States v. Grammatikos*, 633 F.2d 1013, 1019-20 (2d Cir. 1980); *United States v. Miranda*, 526 F.2d 1319 (2d Cir. 1975), *cert. denied*, 429 U.S. 821 (1976).

Leave to Make Further Motions

Defendant's request for leave to make further motions is granted provided that any additional bases for relief are based on facts or information learned by reason of the continuation of the investigation or facts and circumstances revealed in the government's response to the instant motion or this Court's Decision and Order.

Government's Request for Reciprocal Discovery

Since the defendant has moved pursuant to Rule 16(a)(1) of the Federal Rules of Criminal Procedure for similar materials and information, the government is entitled to reciprocal discovery pursuant to Rule 16(b)(1), and its request is hereby granted. The government's motion for advance disclosure of any statement the defendant proposes to use at trial is denied as moot by reason of the requirements contained within Rule 807 of the FRE wherein it is specifically stated:

> a statement may not be admitted under this exception unless the proponent of it makes known to the adverse party sufficiently in advance of the trial or hearing to provide the adverse party with a fair opportunity to prepare to meet it, the proponent's intention to offer the statement and the particulars of it, including the name and address of the declarant.

Therefore, it is hereby **ORDERED** pursuant to 28 U.S.C. § 636(b)(1) that:

This Decision and Order be filed with the Clerk of Court.

ANY OBJECTIONS to this Decision and Order must be filed with the Clerk of this Court within fourteen (14) days after receipt of a copy of this Decision and Order in accordance with the above statute, Fed. R. Crim. P. 58(g)(2) and Local Rule 58.2.

The district judge will ordinarily refuse to consider *de novo*, arguments, case law and/or evidentiary material which could have been, but were not presented to the magistrate judge in the first instance. *See, e.g., Paterson-Leitch Co., Inc. v. Massachusetts Municipal Wholesale Electric Co.*, 840 F.2d 985 (1st Cir. 1988). **Failure to file objections within the specified time or to request an extension of such time waives the right to appeal the District Judge's Order.** *Thomas v. Arn*, 474 U.S. 140 (1985); *Wesolek, et al. v. Canadair Ltd., et al.*, 838 F.2d 55 (2d Cir. 1988).

The parties are reminded that, pursuant to Rule 58.2 of the Local Rules for the Western District of New York, "written objections shall specifically identify the portions of the proposed findings and recommendations to which objection is made and the basis for such objection and shall be supported by legal authority." **Failure to comply with the provisions of Rule 58.2, or with the similar provisions of Rule 58.2 (concerning objections to a Magistrate Judge's Decision and Order), may result in the District Judge's refusal to consider the objection.**

DATED: Buffalo, New York
October 2, 2017

s/ H. Kenneth Schroeder, Jr.
H. KENNETH SCHROEDER, JR.
United States Magistrate Judge